UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/561,234	07/13/2006	Marc Joye	1032326-000315	1646

21839 7590 09/10/2008

BUCHANAN, INGERSOLL & ROONEY PC
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404

EXAMINER	
ABRISHAMKAR, KAVEH	

ART UNIT	PAPER NUMBER
2131	

NOTIFICATION DATE	DELIVERY MODE
09/10/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ADIPFDD@bipc.com

Office Action Summary	Application No.	Applicant(s)	
	10/561,234	JOYE, MARC	
	Examiner	Art Unit	
	KAVEH ABRISHAMKAR	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 December 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-12* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-12* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *12/19/2005*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to the communication filed on December 19, 2005. Claims 1-12 were originally filed for consideration. A preliminary amendment for the claims have been received and considered.

2. Claims 1-12 are currently being considered.

Information Disclosure Statement

3. An initialed and dated copy of the Applicant's IDS form 1449, received on 12/19/2005, is attached to this Office action.

Specification

The following guidelines illustrate the preferred layout for the specification of a utility application. These guidelines are suggested for the applicant's use.

Arrangement of the Specification

As provided in 37 CFR 1.77(b), the specification of a utility application should include the following sections in order. Each of the lettered items should appear in upper case, without underlining or bold type, as a section heading. If no text follows the section heading, the phrase "Not Applicable" should follow the section heading:

(a) TITLE OF THE INVENTION.
(b) CROSS-REFERENCE TO RELATED APPLICATIONS.
(c) STATEMENT REGARDING FEDERALLY SPONSORED RESEARCH OR DEVELOPMENT.
(d) THE NAMES OF THE PARTIES TO A JOINT RESEARCH AGREEMENT.
(e) INCORPORATION-BY-REFERENCE OF MATERIAL SUBMITTED ON A COMPACT DISC.
(f) BACKGROUND OF THE INVENTION.
(1) Field of the Invention.

(2) Description of Related Art including information disclosed under 37 CFR 1.97 and 1.98.
(g) BRIEF SUMMARY OF THE INVENTION.
(h) BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWING(S).
(i) DETAILED DESCRIPTION OF THE INVENTION.
(j) CLAIM OR CLAIMS (commencing on a separate sheet).
(k) ABSTRACT OF THE DISCLOSURE (commencing on a separate sheet).
(l) SEQUENCE LISTING (See MPEP § 2424 and 37 CFR 1.821-1.825. A "Sequence Listing" is required on paper if the application discloses a nucleotide or amino acid sequence as defined in 37 CFR 1.821(a) and if the required "Sequence Listing" is not submitted as an electronic document on compact disc).

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claim 2 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 2 claims that group G is written in additive notation, yet in the independent claim 1, which claims 2 depends from, the group G is written in multiplicative notation. This seems inconsistent and therefore renders the claim indefinite.

Claim Rejections - 35 USC § 102

> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claim 1 is rejected under 35 U.S.C. 102(e) as being anticipated by Clavier et al. (U.S. Patent 7,085,378).

Regarding claim 1, Clavier discloses:

A countermeasure method executed in an electronic component implementing a public-key cryptography algorithm that employs exponentiation computation, with a left-to-right type exponentiation algorithm, of the type y=g d, where g and y are elements of a determined group G written in multiplicative notation, and d is a predetermined number, said countermeasure method including a random draw step, at the start of or during execution of said exponentiation algorithm in deterministic or in probabilistic manner, to mask an accumulator A (column 10, lines 56-67, column 11, lines 1-8: *wherein a random value is drawn to determine which operation will be used, and wherein there are different groups from G1 to G4*).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 2-3, 4, 7, and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Clavier et al. (U.S. Patent 7,085,378) in view of Lambert et al. (U.S. Patent 7,127,063).

Claim 2 is rejected as applied above in rejecting claim 1. Clavier does not explicitly state that the group G is written in an additive notation. Lambert in an analogous art, discloses that in an elliptic curve group, an additive notation can be used instead of the multiplicative group (Lambert: column 5, lines 52-62). Lambert and Clavier are analogous arts as both use elliptic curvy cryptography and Clavier is designed to protect information leakage when performing operations as are performed in Lambert. Therefore, it would been obvious to use the additive or the multiplicative group as disclosed in Lambert, so that generating a secret key and be implemented in any group where the discrete logarithm problem is believed to be intractable (Lambert: column 5, lines 51-54).

Claim 3 is rejected as applied above in rejecting claim 1. Clavier does not explicitly state that the group G is written in a multiplicative notation. Lambert in an analogous art, discloses that in an elliptic curve group, an additive notation can be used or a multiplicative group can be used (Lambert: column 5, lines 52-62). Lambert and Clavier are analogous arts as both use elliptic curvy cryptography and Clavier is designed to protect information leakage when performing operations as are performed in Lambert. Therefore, it would been obvious to use the additive or the multiplicative

group as disclosed in Lambert, so that generating a secret key and be implemented in any group where the discrete logarithm problem is believed to be intractable (Lambert: column 5, lines 51-54).

Claim 4 is rejected as applied above in rejecting claim 3. Furthermore, Lambert discloses:

A countermeasure method according to claim 3, wherein the integer n is equal to 1: n=1 (Lambert: column 23-27: wherein the interval is between 1 and n-1).

Claim 7 is rejected as applied above in rejecting claim 2. Furthermore, Lambert discloses:

A countermeasure method according to claim 2, wherein the exponentiation algorithm applies to the group G of the points of an elliptic curve defined on the finite field GF(qn) (Lambert: column 5, lines 53-62: elliptic curve points).

Claim 12 is rejected as applied above in rejecting claim 1. Furthermore, Clavier discloses:

An electronic component using the countermeasure method according to claim 1(see Abstract: *an electronic component*).

Claims 5, 6, 8-11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Clavier et al. (U.S. Patent 7,085,378) in view of Lambert et al. (U.S. Patent

7,127,063) in further in view of Liardet et al., "Preventing SPA/DPA in ECC Systems using the Jacobi Form."

Claim 5 is rejected as applied above in rejecting claim 4. Clavier-Lambert do not teach the steps: 1) Determine an integer k defining the security of the masking and designate d by the binary representation (d(t), d(t-1), . . . , d(0)) 2) Initialize the accumulator A with the integer 1 3) For i from t down to 0, do the following: 3a) Draw a random .lamda. lying in the range 0 to k-1 and replace the accumulator A with A+.lamda.q (modulo kq) 3b) Replace A with A 2 (modulo kq) 3c) If d(i)=1, replace A with Ag (modulo kq) 4) Return A (modulo q). Liardet discloses the above steps in pages 394-399. It would have been obvious to employ these steps because this method using the Jacobi form has a better defense against SPA attacks (Liardet: page 398, paragraph 4).

Claim 6 is rejected as applied above in rejecting claim 4. Clavier-Lambert do not explicitly disclose the following steps: 1) Determine an integer k defining the security of the masking, and designate d by the binary representation (d(t), d(t-1), . . . , d(0)) 2) Draw a random .lamda. lying in the range 0 to k-1 and initialize the accumulator A with the integer 1+kq (modulo kq) 3) For i from t-1 down to 0, do the following: 3a) Replace A with A2 (modulo kq) 3b) If d(i)=1, replace A with Ag (modulo kq) 4) Return A (modulo q). Liardet discloses the above steps in pages 394-399. It would have been obvious to employ these steps because this method using the Jacobi form has a better defense against SPA attacks (Liardet: page 398, paragraph 4).

Claim 8 is rejected as applied above in rejecting claim 7. Clavier-Lambert do not explicitly disclose the following steps: 1) Initialize the accumulator A=(A.sub.x,A.sub.y,A.sub.z) with the (x,y,1) triplet and designate d by the binary signed-digit representation (d(t+1), d(t), . . . , d(0)) with d(t+1)=1 2) For i from t down to 0, do the following: 2a) Draw a random non-zero element .lamda. from GF(qn) and replace the accumulator A=(A.sub.x,A.sub.y,A.sub.z) with (.lamda.2A.sub.x, .lamda.3A.sub.y, .lamda.A.sub.z) 2b) Replace A=(A.sub.x,A.sub.y,A.sub.z) with 2*A=(A.sub.x,A.sub.y,A.sub.z) in Jacobian representation, on the elliptic curve 2c) If d(i) is non-zero, replace A=(A.sub.x,A.sub.y,A.sub.z) with (A.sub.x,A.sub.y,A.sub.z)+d(i)*(x)y,1) in Jacobian representation on the elliptic curve 3) If A.sub.z=0, return the point at infinity; otherwise return (A.sub.x/(A.sub.z)2, A.sub.y/(A.sub.z)3). Liardet discloses the above steps in pages 394-399. It would have been obvious to employ these steps because this method using the Jacobi form has a better defense against SPA attacks (Liardet: page 398, paragraph 4).

Claim 9 is rejected as applied above in rejecting claim 7. Clavier-Lambert do not explicitly disclose the following steps: 1) Draw a non-zero random element .lamda. from GF(qn) and initialize the accumulator A=(A.sub.x,A.sub.y,A.sub.z) with the (.lamda.2x, .lamda.3y, .lamda.) triplet and designate d by the binary signed-digit representation (d(t+1), d(t), . . . , d(0)) with d(t+1)=1 2) For i from t down to 0, do the following: 2a) Replace A=(A.sub.x,A.sub.y,A.sub.z) with 2*A=(A.sub.x,A.sub.y,A.sub.z) in Jacobian

representation, on the elliptic curve 2b) If d(i) is non-zero, replace A=(A.sub.x,A.sub.y,A.sub.z) with (A.sub.x,A.sub.y,A.sub.z)+d(i)*(x,y,1) in Jacobian representation on the elliptic curve 3) If A.sub.z=0, return the point at infinity; otherwise return (A.sub.x/(A.sub.z)2, A.sub.y/(A.sub.z)3). Liardet discloses the above steps in pages 394-399. It would have been obvious to employ these steps because this method using the Jacobi form has a better defense against SPA attacks (Liardet: page 398, paragraph 4).

Claim 10 is rejected as applied above in rejecting claim 7. Clavier-Lambert do not explicitly disclose the following steps: 1) Initialize the accumulator A=(A.sub.x,A.sub.y,A.sub.z) with the (x,y,1) triplet and designate d by the binary signed-digit representation (d(t+1), d(t), . . . , d(0)) with d(t+1)=1 2) For i from t down to 0, do the following: 2a) Draw a random non-zero element .lamda. from GF(qn) and replace the accumulator A=(A.sub.x,A.sub.y,A.sub.z) with (.lamda.A.sub.x, .lamda.A.sub.y, .lamda.A.sub.z) 2b) Replace A=(A.sub.x,A.sub.y,A.sub.z) with 2*A=(A.sub.x,A.sub.y,A.sub.z) in homogeneous representation, on the elliptic curve 2c) If d(i) is non-zero, replace A=(A.sub.x,A.sub.y,A.sub.z) with (A.sub.x,A.sub.y,A.sub.z)+d(i)*(x,y,1) in homogeneous representation on the elliptic curve 3) If A.sub.z=0, return the point at infinity; otherwise return (A.sub.x/A.sub.z, A.sub.y/A.sub.z). Liardet discloses the above steps in pages 394-399. It would have been obvious to employ these steps because this method using the Jacobi form has a better defense against SPA attacks (Liardet: page 398, paragraph 4).

Claim 11 is rejected as applied above in rejecting claim 7. Clavier-Lambert do not explicitly disclose the following steps: 1) Draw a non-zero random element .lamda. from GF(qn) and initialize the accumulator A=(A.sub.x,A.sub.y,A.sub.z) with the (.lamda.x, .lamda.y, .lamda.) triplet and give d by the binary signed-digit representation (d(t+1), d(t), . . . , d(0)) with d(t+1)=1 2) For i from t down to 0, do the following: 2a) Replace A=(A.sub.x,A.sub.y,A.sub.z) with 2*A=(A.sub.x,A.sub.y,A.sub.z) in homogeneous representation, on the elliptic curve 2b) If d(i) is non-zero, replace A=(A.sub.x,A.sub.y,A.sub.z) with (A.sub.x,A.sub.y,A.sub.z)+d(i)*(x,y,1) in homogeneous representation on the elliptic curve 3) If A.sub.z=0, return the point at infinity; otherwise return (A.sub.x/A.sub.z, A.sub.y/A.sub.z). Liardet discloses the above steps in pages 394-399. It would have been obvious to employ these steps because this method using the Jacobi form has a better defense against SPA attacks (Liardet: page 398, paragraph 4).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to KAVEH ABRISHAMKAR whose telephone number is (571)272-3786. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Kaveh Abrishamkar/
Examiner, Art Unit 2131

/K. A./
09/05/2008
Examiner, Art Unit 2131